UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/856,813	08/21/2001	John Desborough Yesburg	1376-010862	3464

7590 06/03/2005

EXAMINER
COLIN, CARL G

ART UNIT	PAPER NUMBER
2136	

Webb Ziesenheim Logsdon
Orkin & Hanson
700 Koppers Building
436 Seventh Avenue
Pittsburgh, PA 15219-1818

DATE MAILED: 06/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/856,813	YESBURG, JOHN DESBOROUGH	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 March 2005* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☒ The proposed drawing correction filed on *09 March 2005* is: a)☒ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 3/9/2005, applicant amends claims 1-7, 9, 11, 14, 17, 20, and 22. The following claims 1-23 are presented for examination.

2. Applicant's arguments, pages 7-8, filed on 3/9/2005, with respect to the rejection of claims 1-23 have been fully considered, but they are not persuasive. The use of asymmetric cryptography and symmetric cryptography are well known in the art as disclosed in applicant's background and Bruce Schneier's document. Applicant has amended the independent claims to include a trusted display. Upon further consideration, a new ground of rejection is made in view of Veil, who discloses a trusted display to guarantee that information displayed is true information. Therefore, independent claim 1 is rejected in view of Wang and Veil.

Specification

3. The abstract of the disclosure is objected to because of the first sentence "disclosed is" the usage of phrases such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc. should be avoided. Correction is required. See MPEP § 608.01(b).

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the

printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

3.1 The amendment filed 3/9/2005 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: "and prevents the user from being tricked into signing one document when he believes he is signing another", page 2 of 16 of the amendment.

Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4.1 Claims 4-6, 8, 10, 11, 16-18, 21-23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 4 and 5 recite the limitation "said cryptographic engine process". There is insufficient antecedent basis for this limitation in the claim.

Claim 6 recites the limitation " wherein said digital private key protection device further comprises a private key protection device private key storage means wherein digital data sired by said private key protection device after operation of said user operable input means is further signed by said private key of said private key protection device". This limitation fails to point out an antecedent basis with the private key protection device, digital private key protection device, and private key, digital private key. The disclosure does not disclose a difference between a digital private key protection device or private key protection device nor private key and digital private key. There is insufficient antecedent basis for this limitation in the claim.

Claims 8 and 10 recite the limitation "said display". There is insufficient antecedent basis for this limitation in these claims.

Claims 11, 16-18, 21-23 recite the limitation "said display". Claim 23 recites the limitation the private key protection device. There is insufficient antecedent basis for this limitation in these claims.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at

the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.1 **Claims 1, 4-8, 10, 14, 17-23** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,917,913 to **Wang** in view of US Patent 6,092,202 to **Veil et al**.

5.2 **As per claim 1, Wang** discloses a digital private key protection device, comprising a digital private key storage means containing a user's digital private key, for example (see column 9, lines 5-20); a cryptographic engine, for example (see column 9, lines 1-6); a communications port for receiving digital data from an external device, and for transmitting data to said external device, for example (see column 9, lines 20-40); a display means for displaying said received digital data, for example (see column 10, line 65 through column 11, 12); a user operable input means connected to said cryptographic engine to indicate when operated by said user their approval of said displayed received digital data, for example (see column 11, lines 14-41, column 10, lines 36-67); wherein said cryptographic engine is trusted to only apply said user's digital private key to sign said received data only if said user operable input means is operated and communicate said signed data external of said digital private key protection device, for example (see column 11, lines 33-62 and column 4, lines 40-65). **Wang** does not explicitly disclose a trusted display. **Veil et al** in an analogous art discloses a trusted display for displaying true transaction information (see abstract). **Veil et al** discloses that the present invention displays transaction information that has been authenticated as true transaction information; and

the trusted display can optionally be separate so that the user can visually see a conflict between a correct and false transaction and alerts user to a possible tampering or attack (column 7, line 50 through column 8, line 33). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the display of **Wang** to provide the user with a trusted display that displays transaction information that has been authenticated as true transaction information; and the trusted display can optionally be separate so that the user can visually see a conflict between a correct and false transaction and alerts user to a possible tampering or attack as taught by **Veil et al**. One of ordinary skill in the art would have been lead to make such a modification to guarantee that a transaction displayed represents the true information as suggested by **Veil et al** (column 7, line 50 through column 8, line 33).

As per claim 4, Wang discloses the limitation of an audit means that meets the recitation of wherein signed data is not transmitted external of said digital private key protection device until a said encryption process is audited by said audit means, for example (see column 7, lines 1-17 and column 12, lines 35-50; column 4, lines 40-55).

As per claim 5, Wang discloses the limitation of an audit means that meets the recitation of wherein signed data is not displayed until a said encryption process is audited by said audit means, for example (see column 7, lines 1-17 and column 12, lines 35-50).

As per claim 6, Veil et al discloses verifying an issuer's signature on a certificate using the protection device that meets the recitation of wherein digital data signed by said private key

protection device is further signed by said private key of said private key protection device (column 12, lines 14-30). Therefore, claim 6 is rejected on the same rationale as the rejection of claim 1.

As per claims 7-8, Veil et al discloses use of public/private key for decrypting at the other hand using either public or private key (column 5, lines 48 through column 6, line 16 and discloses trusted display for verification (claim 1). Therefore, claims 7-8 are rejected on the same rationale as the rejection of claim 1.

As per claim 10, Wang discloses the limitation of wherein said cryptographic engine is trusted to decrypt digital data using said user's digital private key and passing decrypted digital data to said display means for display of said received digital data, for example (see column 7, lines 42-61).

As per claim 14, Veil et al discloses wherein said digital private key storage means also contains a digital shared secret symmetric key wherein said cryptographic engine is trusted to only apply said digital shared secret symmetric key to encrypt data only if said user operable input means is operated and also trusted to communicate said encrypted data external of said digital private key protection device (column 5, line 55 through column 6, line 16 and column 11, line 29-67). **Veil et al** discloses a user PIN to unlock the private key and authorizes use of sensitive data if verified that meets the recitation of user operable input means. Wang also

discloses another input means using a switch. Therefore, claim 14 is rejected on the same rationale as the rejection of claim 1.

As per claims 17-21, the combination of **Wang and Veil et al** discloses the limitation of wherein said trusted display means is external to said device and controlled by said device for displaying data transmitted from said communications port in a trusted manner wherein said digital private key storage means is removable from said device (see Veil, column 7, lines 58-60 and drawings); wherein said user operable input means is external to said device and controlled by said device to be actuated by said user in a predetermined manner; further comprising identification and authentication means actuated by said user in a predetermined manner; an audit means which audits said actuation of said user operable input means (Wang, column 4, lines 40-67 and column 10, line 55 through column 11).

As per claims 22-23, the combination of **Wang and Veil et al** discloses a digital private key protection device according to claim 1, wherein a cryptographic request is received from said external device according to a predetermined application programming interface, such that the request is performed by said digital private key protection device using the user's private or other keys as identified by the request, but excluding the private key protection device with the result being transmitted to said external device or a predetermined destination included in said request or otherwise predetermined, wherein said device displays a description of said request to the user and, only if the user operates said user operable input means, does said device carry out said request (column 11, lines 33-67).

6. **Claims 2, 3, 9, and 15-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,917,913 to **Wang** in view of US Patent 6,092,202 to **Veil et al** as applied to claim 1 and further in view of **Bruce Schneier**, Applied Cryptography, 1996, John Wiley & Sons, Second Edition, Pages 43-44.

6.1 **As per claims 2, 3, 9, and 15-16, Wang** substantially teaches the claimed method of claim 1 and discloses that the invention is not limited to any encryption scheme, for example (see column 5, lines 35-50). **Wang** discloses that the received data can be encrypted using a trusted public and private key, for example (see column 7, lines 18-67). **Veil et al** discloses proving electronic transactions performed by a cardholder and discloses verifying whether a user is authorized to conduct a transaction to prevent repudiation (column 11, line 45 through column 12, line 14 and columns 5-6); and further discloses a trusted display for verification of transaction information as discussed above in claim 1. **Veil et al** discloses transaction data including a certificate created using a user's private key (column 11, lines 22-45). The limitation of received data that includes instructions to determine which protocol to use to communicate or keys to use for encryption is well known in packet processing and can be also found in Schneier textbook. Neither of the references explicitly teaches validating signature of a user's public key from a plurality of public keys and decrypts data using the verified public key. **Schneier** in an analogous art teaches a key certification authority wherein the users' public keys are signed with a trusted private key to prevent attack against public key, for example (see pages 43, 62-64); and further discloses validating signature of said user's public key with said trusted public key to

determine the veracity of said user's public key and then decrypts said received data using said verified predetermined user's public key, for example (see pages 43, 62-64). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to store user's public keys and have the public keys signed by a trusted private key using public/private key pairs as taught by **Schneier**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Schneier** to have a card that can be used by more than one user and prevent attack against public key and prevents users from repudiation as it proves proof of user's participation.

7. **Claims 11-13** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,917,913 to **Wang** in view of US Patent 6,092,202 to **Veil et al** as applied to claim 1 and further in view of US Patent 5,742,756 to **Dillaway et al**.

7.1 **As per claim 11-13, Wang** discloses a user may activate a button to create a transaction approval and message encrypted or decrypted to be transmitted unless said user operable input means is operated (column 11, lines 40-55). **Veil et al** discloses encryption decryption of transaction and further discloses sensitive data remains resident in protected device (column 11, lines 1-8). Neither of the references explicitly states decrypted information is not released external to said device unless said user operable input means is operated. **Dillaway et al** in an analogous art teaches security and authentication and digital signature performed by a smart card and discloses to provide a higher degree of security users can be required to provide password or

wait for user presence signal before performing any security critical operations (column 5, line 50 through column 6, line 30). Transmitting decrypting information outside of the card is a security critical operation to one skilled in the art. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to activate the approval button of Wang before decrypted information is released external to said device to confirm the presence of the user as taught by **Dillaway et al**. One of ordinary skill in the art would have been lead to make such a modification to confirm the presence of the user before performing a security critical operation as suggested by **Dillaway et al** (column 5, line 50 through column 6, line 30).

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8.1 The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art protection device to protect private keys of users and several cryptographic schemes to verify signatures and key used. Many of the claimed features are disclosed in these references.

US Patents: 4,529,870 Chaum;; 4,731,842 Smith; 6,212,635 Reardon; 6,484,260 Scott et al; 6,018,724 Arent; 6,507,909 Zurko et al.

8.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Carl Colin
Patent Examiner
May 27, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100